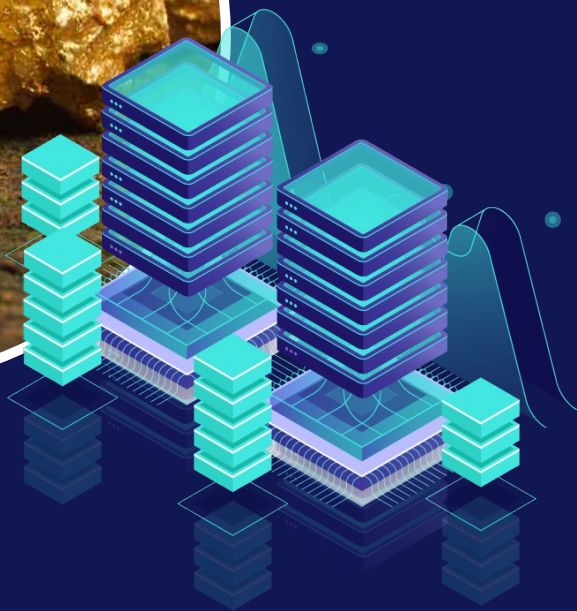
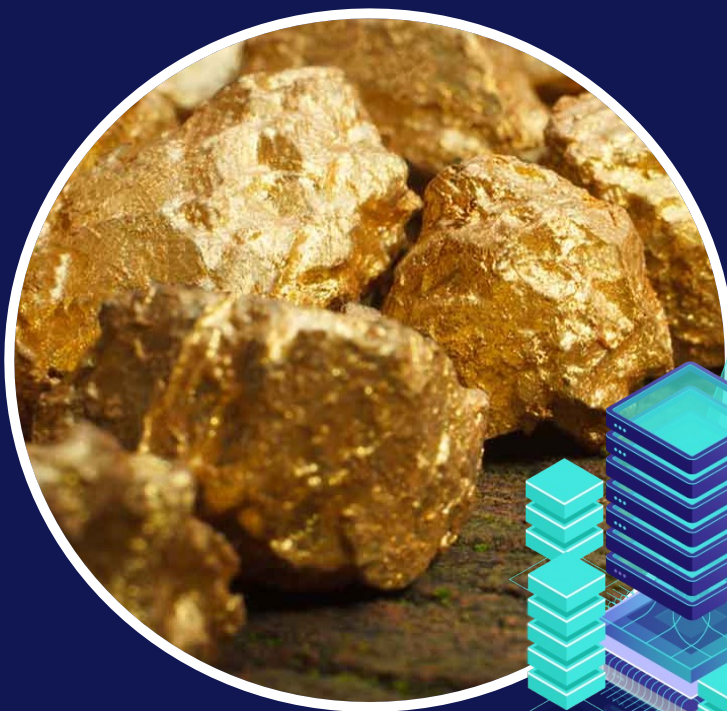


ИСТОРИИ УСПЕХА

Маkves DСАР помогает оптимизировать работу службы информационной безопасности полиметаллического холдинга «Селигдар»



Отрасль:
Горнодобывающая
промышленность




Компания

История полиметаллического холдинга «Селигдар» начинается с 1975 года. Сегодня компания объединяет активы золотодобывающих предприятий, осуществляющих деятельность в Республике Саха, Республике Бурятия, Алтайском крае и Оренбургской области, а также активы оловодобывающих предприятий в Хабаровском крае и на Чукотке. Фундаментом успеха компании служат технологическая и финансовая эффективность – компания непрерывно работает над повышением эффективности за счет использования наиболее передовых технологий и совершенствования бизнес-процессов.

Задача

Информация, которую сотрудники компании генерируют и используют в своей работе, хаотично перемещается в рамках корпоративной сети. Объем этой информации стремительно растет. Сотрудники ежедневно пользуются привычными для них инструментами: они создают копии личных данных или сохраняют почтовую переписку на файловых хранилищах. В случае увольнения или перевода в другое подразделение часто забывается, что при изменении должностных обязанностей необходимо поменять и уровень доступа к информационным ресурсам. В результате чего важная для бизнеса информация может оказаться под угрозой компрометации.

«Только в московском подразделении холдинга находится более 800 тысяч файлов, которые содержат информацию об отчислениях в пенсионные фонды, финансовые документы и данные разведки. Их потеря может грозить остановкой производства и других важных бизнес-процессов», – рассказывает Евгений Зайцев, начальник управления информационной безопасности Дирекции по безопасности ГК «Селигдар».



Экспансивное развитие ИТ-инфраструктуры породило большое количество систем с «понятийным» администрированием – общие файловые ресурсы, несколько доменов и так далее, что закономерно привело к неуправляемому хаосу. Попытки разобраться «вручную» показали, что задача решаемая, но сроки и объем трудозатрат абсолютно неприемлемы. В связи с чем начался поиск средства автоматизации для контроля над неструктурированными данными.

«Есть 2 варианта борьбы с хаосом, – комментирует Евгений Зайцев. – Можно создать новое файловое хранилище, работа с которым будет осуществляться строго в соответствии с регламентом безопасности. Однако при переносе информации в новое хранилище, могут быть потеряны данные, критичные для производства и других бизнес-процессов. К тому же решение задачи таким путем требует много человеческих ресурсов. Географически распределенная инфраструктура компании предполагает круглосуточную активность сотрудников, и только для мониторинга соблюдения регламента необходимо будет задействовать нескольких специалистов по информационной безопасности. Второй, и наиболее эффективный вариант – это автоматизация».



Решение Makves

Чтобы обеспечить контроль над корпоративной информацией, правами и действиями пользователей компанией было принято решение о внедрении системы класса DCAP (Data-Centric Audit and Protection).

«При выборе системы мы ориентировались на отечественные решения, готовые предоставить инструмент в соответствии с нашими запросами и обеспечить оперативную техническую поддержку на русском языке. Интегратор сразу предложил Makves DCAP – другие решения не в полной мере отвечали нашим требованиям, были дороже и требовали больше ресурсов для тестирования и развертывания системы», – пояснил Евгений Зайцев.

С помощью решения Makves в управлении по информационной безопасности автоматизировали процесс анализа файловых ресурсов и пользователей. Специалисты используют Makves DCAP для непрерывного контроля полномочий и прав доступа к информационным ресурсам, выявления избыточного доступа к документам, имеющим ограничительную отметку, выявления дубликатов файлов и оптимизации файловых хранилищ.

В процессе опытной эксплуатации было выявлено и заблокировано 30 учетных записей ранее уволенных сотрудников и ограничены полномочия у 100 сотрудников в соответствии с их должностными обязанностями; был ограничен доступ к более чем 50 папкам, содержащим порядка 700 документов, попадающих в категорию «Коммерческая тайна» и «Персональные данные». Система позволила выявить более 1 терабайта неиспользуемых копий файлов на главном файловом сервере компании и оптимизировать общий объем файловых хранилищ на 20%.

«Только первичный аудит двух хранилищ выявил более двух миллионов файлов, – рассказывает Евгений Зайцев, – обработка которых вручную могла бы занять порядка 14 тысяч человеко-часов без учета динамики роста данных, связанных с копированием, удалением, созданием новых документов, открытием/закрытием доступа и так далее».

Повысив прозрачность информационных ресурсов, ИБ-специалисты компании получили возможность оперативно принимать меры для предотвращения инцидентов информационной безопасности и обеспечения непрерывности процессов производства на предприятиях холдинга.

География проекта



РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ

Оптимизация ИБ и ИТ ресурсов

- Автоматизация процессов позволила избежать расширения штата сотрудников информационной безопасности и увеличения фонда оплаты труда. Что помогло компании сохранить до 4-х миллионов рублей в год.
- Специалистам больше не нужно тратить время на поиск уязвимостей, связанных с хранением и доступом к данным. Теперь они могут сосредоточиться на других не менее важных задачах, таких как развитие систем обеспечения информационной безопасности, внедрение новых решений и модернизация существующих.
- Оптимизация файловых хранилищ позволила отложить необходимость в приобретении нового дорогостоящего оборудования для хранения данных.

Снижение рисков информационной и экономической безопасности

- Внедрение Makves DCAP позволило значительно сократить количество инцидентов, связанных с «пропажей» файлов, незаблокированными учетными записями уволенных сотрудников и чрезмерным доступом к информационным ресурсам компании.



**УЗНАЙТЕ, КАК ПРОДУКТЫ MAKVES
ПОМОГУТ РЕШИТЬ ВАШИ ЗАДАЧИ!**

[Запишитесь на демо](#)

Инженер MAKVES продемонстрирует возможности системы на примере типовой ИТ-инфраструктуры и ответит на все ваши вопросы.



Узнать больше
<https://makves.ru/dcap>



Заказать тест
<https://makves.ru/free-trial>